The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

09/14/2016

SUBJECT:

Multiple Vulnerabilities in MySQL, PerconaDB, and MariaDB Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in MySQL, MariaDB, and PerconaDB with the most severe of which could allow for arbitrary code execution. MySQL is a relational database management system that is used to correlate and organize data. MariaDB and PerconaDB are clones of MySQL.

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with user rights of database service.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- MySQL versions 5.5.51 and earlier
- MySQL versions 5.6.33 and earlier
- MySQL versions 5.7.11 and earlier
- MariaDB versions prior to 5.5.51
- MariaDB versions prior to 10.0.27
- MariaDB verions prior to 10.1.17
- PerconaDB versions prior to 5.5.51-38.1
- PerconaDB versions prior to 5.6.32-78.0

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

MySQL is prone to a remote code execution vulnerability which may allow an attacker to execute arbitrary code with user rights of the database service. This vulnerability is exploited by an attacker manipulating a "my.cnf" configuration file to include an arbitrary library at the start of MySQL database service. When MySQL is restarted, the arbitrary library can be used by the attacker to execute code with MySQL root user privileges. (CVE-2016-6662)

In addition, MySQL is also prone to a security bypass vulnerability that would allow attackers to create a "/var/lib/mysql/my.cnf" file without the FILE privilege requirement. (CVE-2016-6663)

(Note: MS-ISAC will provide updates about CVE-2016-6663 as more information becomes available. In addition, only MariaDB and PerconaDB currently have patches at this time.)

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by MariaDB and PerconaDB to vulnerable systems immediately after appropriate testing.
- Apply appropriate updates provided by Oracle for MySQL once they are available.
- Unless there is a critical and documented business need, do not allow access to the database from external sources by blocking the appropriate port at the perimeter firewall.
- Configuration files should be checked to ensure that access to the database is restricted to authorized hosts.
- Restrict permissions of the user account associated with database service so that it only has read access to the configuration file.

REFERENCES:

LegalHackers:
http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html

Percona:
https://www.percona.com/blog/2016/09/12/percona-server-critical-update-cve-2016-6662/

MariaDB:
https://mariadb.org/mariadb-server-versions-remote-root-code-execution-vulnerability-cve-2016-6662/

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6662
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6663